* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] When accessing the service currently provided with the local network side from the device by the side of global network, The authentication means which is the network connection control device which performs control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, An access-permission entry creation means to generate an access-permission entry and to add the access-permission entry concerned to an access permit list to the access request of the device attested by the above-mentioned authentication means, When a data packet is received from the device by the side of the above-mentioned global network, The network connection control unit which has the control means which judges whether the data packet concerned is transmitted to a local network side based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list.
[Claim 2] The above-mentioned entry creation means is a network connection control unit according to claim 1 which generates the access-permission entry which extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and contains a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.
[Claim 3] The above-mentioned control means is a network connection control unit according to claim 1 which transmits the data packet concerned to a local network side when a transmitting agency IP address, a port number and a destination IP address, and a port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, a destination IP address, a transmitting agency port number, and a destination port number are in agreement.
[Claim 4] The above-mentioned control means is a network connection control unit according to claim 1 which deletes the access-permission entry corresponding to the access concerned from the above-mentioned access permit list according to the access termination directions from the device by the side of the above-mentioned global network.
[Claim 5] The above-mentioned control means is a network connection control unit according to claim 1 which deletes the access-permission entry concerned from the above-mentioned access permit list when the elapsed time from the last access is computed and the elapsed time concerned exceeds the conventional time set up beforehand based on the last access-permission time of day corresponding to the receipt time of the data packet transmitted from the device by the side of the above-mentioned global network memorized by the access-permission entry.
[Claim 6] The network connection control unit according to claim 1 which has further a storage means to memorize the above-mentioned access permit list.
[Claim 7] When accessing the service currently provided with the local network side from the device by the side of global network, The step which is the network connection control approach of performing control which permits or refuses the access concerned, and attests to the device by the side of the above-

mentioned global network, The step which generates an access-permission entry and adds the access-permission entry concerned to an access permit list to the access request of the device by which authentication was carried out [above-mentioned], When a data packet is received from the device by the side of the above-mentioned global network, The network connection control approach of having the step which judges whether the data packet concerned being transmitted to a local network side based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list.

[Claim 8] The network connection control approach according to claim 7 which generates the access-permission entry which extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned] when generating the above-mentioned access-permission entry, and contains a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.

[Claim 9] The network connection control approach according to claim 7 of transmitting the data packet concerned to a local network side when a transmitting agency IP address, a transmitting agency port number, a destination IP address, and a destination port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, the IP address of the destination, a transmission place port number, and a destination port number are in agreement.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the control unit which controls the access permission, and its control approach, when accessing the service currently offered by the local network side from the device by the side of global network.
[0002]
[Description of the Prior Art] The service establishments which a network user increases rapidly with the spread of network, and offer various information data on a network are increasing in number. While the convenience which can obtain required information easily using a network increases, it has been the problem for a network manager that the damage by unjust access is big. They are the server by which the gateway equipped with authorization or the fire wall function which controls carrying out disapproval etc. is connected to the local network in access to the local network called LAN (Local Area Network) from the global network called WAN (Wide Area Network), for example, the Internet etc., and a means effective in securing the security of a terminal equipment.

[0003] Usually, when accessing to the network device prepared on a certain specific global network from the local network, for example, the server which offers a certain specific information, it carries out through the gateway connected between global network and a local network. In the gateway concerned, the global address used for global network and the local address used for a local network are assigned, respectively, and also the communication link port for performing data communication is given between the terminal equipments connected to global network and a local network.

[0004] In order to prevent unjust access from a global-network side, such as the Internet, the fire wall prepared in the gateway is performed according to the individual according to the setup on a system in the control which permits or forbids each access from the Internet side. By this setup, all accesses are forbidden by the default except the access place permitted specially. By this, unjust access from the outside can destroy the resource in terminal equipments, such as each server on a local network, or leakage of a secret matter etc. can be prevented.

[0005] However, since just access is also refused by having taken such a measure, a result it becomes impossible to provide a general user with the comfortable Internet service freely and by which the convenience of service is spoiled may be brought.

[0006] Maintaining the security nature of a local network, access from the outside was distinguished simply, unjust access was forbidden, and the amelioration technique of the fire wall which permits just access was proposed. For example, such an amelioration technique is indicated in the open patent official report "JP,11-338799,A" which is patent reference. When the device by the side of global network accesses the device by which the fire wall is prepared, for example, the server which offers predetermined data utility, (this is hereafter called a local server) according to the technique indicated with this reference, the migration code for accessing that local server is first downloaded from the gateway of that local network. And the downloaded migration code is accessed to a local server via the junction agent generated by performing by its own device.

[0007] It is possible to raise the convenience of access to a local server from global network, maintaining security level equivalent to the conventional fire wall by adopting this approach.
[0008]
[Problem(s) to be Solved by the Invention] By the way, in order to download a migration code in advance, and to perform this migration code and to generate a junction agent in case a local server is accessed when using the technique mentioned above, there is disadvantageous profit that the environment where a migration code is performed must be prepared beforehand.
[0009] This invention is made in view of this situation, the purpose is permitted to the device which had access to the device on a local network from global network attested, and it is in offering the network connection control unit which can control an authorization setup of access automatically, and its control approach.
[0010]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the network connection control unit of this invention When accessing the service currently provided with the local network side from the device by the side of global network, The authentication means which is the network connection control device which performs control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, An access-permission entry creation means to generate an access-permission entry and to add the access-permission entry concerned to an access permit list to the access request of the device attested by the above-mentioned authentication means, When a data packet is received from the device by the side of the above-mentioned global network, Based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list, it has the control means which judges whether the data packet concerned is transmitted to a local network side.
[0011] Moreover, in this invention, suitably, the above-mentioned entry creation means extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and generates the access-permission entry containing a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.
[0012] Moreover, in this invention, suitably, the above-mentioned control means transmits the data packet concerned to a local network side, when a transmitting agency IP address, a port number and a destination IP address, and a port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, a destination IP address, a transmitting agency port number, and a destination port number are in agreement.
[0013] Moreover, in this invention, the above-mentioned control means deletes the access-permission entry corresponding to the access concerned from the above-mentioned access permit list suitably according to the access termination directions from the device by the side of the above-mentioned global network.
[0014] Moreover, in this invention, suitably, the above-mentioned control means computes the elapsed time from the last access based on the last access-permission time of day corresponding to the receipt time of the data packet transmitted from the device by the side of the above-mentioned global network memorized by the access-permission entry, and when the elapsed time concerned exceeds the conventional time set up beforehand, it deletes the access-permission entry concerned from the above-mentioned access permit list.
[0015] Moreover, the network connection control approach of this invention When accessing the service currently provided with the local network side from the device by the side of global network, The step which is the network connection control approach of performing control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, When a data packet is received to access of a device by which authentication was carried out [above-

mentioned] from the step which generates an access-permission entry and adds the access-permission entry concerned to an access permit list, and the device by the side of the above-mentioned global network, Based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list, it has the step which judges whether the data packet concerned is transmitted to a local network side.

[0016] Moreover, in this invention, suitably, when generating the above-mentioned access-permission entry, access information is extracted from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and the access-permission entry containing a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day is generated.

[0017] Furthermore, in this invention, when a transmitting agency IP address, a transmitting agency port number, a destination IP address, and a destination port number are suitably extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, the IP address of the destination, a transmission place port number, and a destination port number are in agreement, the data packet concerned is transmitted to a local network side.

[0018]

[Embodiment of the Invention] 1st operation gestalt drawing 1 is the block diagram showing an example of the network system containing the network connection control unit concerning this invention. This network system is constituted like illustration by the gateway 30 connected between global network (WAN:Wide Area Network) 10, a local network (LAN:Local Area Network) 20, global network 10, and a local network, the terminal equipment 40 connected to global network 10, and the terminal equipment 50 connected to the local network 20.

[0019] The gateway 30 is the so-called network connection control unit which has the fire wall function to permit the access, only to the attested terminal equipment, when the access request to the service from the terminal equipment by the side of global network 10 currently offered by the local network 20 side is received. In addition, although one terminal equipment is connected to global network 10 and a local network 20 at a time in drawing 1 , respectively, many terminal equipments are usually connected to global network 10 and a local network 20 in the actual network system, respectively.

[0020] The fire wall is prepared in the gateway 30 and access to the terminal equipment by the side of a local network 20 by the side of global network 10 from a terminal equipment is not permitted in usual. Moreover, inside the local network 20, the respectively private IP address is assigned to each terminal equipment, and at least one global IP address is assigned to the global-network connection interface of the gateway 30. Each terminal equipment by the side of a local network 20 accesses the service which a global-network side offers using an IP masquarade technique.

[0021] By the access request from the device attested among the terminal equipments connected to global network 10 by the network system constituted in this way, this invention permits access to the service by the side of the local network 20 which specified only the device, refuses access from the device by the side of other global network, namely, offers the network connection control unit which can be changed dynamically for a fire wall setup.

[0022] In addition, in the following explanation, the message at the time of notifying to the gateway 30 giving [which the terminal equipment by the side of global network 10 wishes] is called "service access demand message" for convenience. Moreover, in the local network 20 side, since the private IP address is used, the port number is assigned to the gateway 30 for every service so that the service currently offered by the local network 20 side can be specified from the device by the side of global network. The device by the side of global network 10 can access giving [to wish one's service] by specifying the global IP address and port number of the interface by the side of the global network in the gateway 30.

[0023] Here, when the device by the side of a "service IP address", a "service port number", a call, and global network accesses an IP address and a port number for the device by the side of global network to specify the service by the side of a local network for convenience at the device by the side of a local

network, respectively, these service IP addresses and service port numbers are included in a service access demand message, and it transmits to the gateway 30.
[0024] Drawing 2 is the block diagram showing the configuration of the gateway 30. Hereafter, the configuration and function of each part of the gateway 30 are explained, referring to drawing 2 . The gateway 30 is constituted by the access-control section 31, the address translation section 32, the global-network (WAN) side interface section 33, the local network (LAN) side interface section 34, and the storage section 35 like illustration. Furthermore, the access section 31 is constituted by the analysis section 301, the authentication section 302, and the list Management Department 303.
[0025] The access-control section 31 analyzes the service access demand message which received from the global-network side, attests a device, and manages an access permit list. Moreover, according to the result of the analysis and authentication, the authorization or refusal of access of a data packet received from the global-network side is controlled.
[0026] Hereafter, each component of the access-control section 31 is explained. The analysis section 301 analyzes by extracting required information from the data packet which received by the WAN side interface section 33. For example, if a service access demand message is transmitted from the device by the side of global network to the device by the side of a local network, this message will receive by the WAN side interface section 33, and will be passed to the access-control section 31. In the access-control section 31, from the service access demand message which received, information, such as a transmitting agency IP address, a port number and a destination IP address, and a port number, is extracted by the analysis section 301, an access-permission entry is generated based on it, and it is sent to the list Management Department 303.
[0027] Moreover, the analysis section 301 extracts information, such as an IP address of a transmitting agency and the destination, and a port number, from the header of a data packet received by the WAN side interface section 33, and opts for authorization or refusal of access based on the extracted information concerned and the information on the access-permission entry contained in an access permit list.
[0028] The authentication section 302 attests according to the authentication approach and authentication procedure which were beforehand set up to the device concerned, when a service access demand message is received from the device by the side of global network 10. And the information about the attested device is transmitted to the analysis section 301, and the access-permission entry to the access is created by the analysis section 301.
[0029] The list Management Department 303 adds the access-permission entry created by the analysis section 301 to reception and the access permit list memorized by the storage section 35. Or when access termination is carried out, the access-permission entry corresponding to the access is deleted from the access permit list memorized by the storage section 35.
[0030] The address translation section 32 is required only when the private IP address (or it is called a local IP address) is used for the local network 20 side. That is, the address translation section 32 changes the global IP address currently used by the global-network 10 side, and the local IP address currently used by the local network 20 side.
[0031] The WAN side interface 33 transmits and receives a packet to global network 10. That is, the packet transmitted from global network 10 is received, and the packet generated by the access-control section 31 by delivery and the access-control section 31 is transmitted to global network 10.
[0032] The LAN side interface 34 transmits and receives a packet to a local network 20. That is, the packet transmitted from the local network 20 is received, and the packet sent to the address translation section 32 from delivery and the address translation section 32 is transmitted to a local network 20.
[0033] The storage section 35 memorizes an access permit list. The access permit list concerned is managed by the list Management Department, the access-control section 31. The access-permission entry of access which the access-permission entry generated by the analysis section 301 was added to the access permit list concerned, and was ended is deleted from the access permit list concerned.
[0034] Hereafter, actuation of the access-control section 31 of the gateway 30 in this operation gestalt is explained. First, from the device by the side of global network 10, when the "service access demand

message" the "service IP address" and the "service port number" were indicated to be is received from the WAN side interface section 33, actuation of the access-control section 31 is explained.

[0035] Drawing 3 is a flow chart which shows actuation of the access-control section 31 when receiving a "service access demand message." As shown in drawing 3 , the service access demand message which received from the WAN side interface section 33 is received first (step S1). And the starting point IP address and starting point port number which show the device and interface of the transmitting side indicated by received IP header of a service access demand message are checked, and it attests about the device which transmitted the service access demand message concerned (step S2). In addition, by this invention, although the approach of attesting a device can consider authentication by IPsecAH, the 3rd person authentication by Kerberos, etc., since it is realizable by the existing approach, authentication of this transmitting-side device is not limited especially here.

[0036] When authentication goes wrong, the "service access demand message" is discarded (step S3), and processing is ended. Conversely, when it succeeds in authentication, processing shown below is performed.

[0037] When authentication is successful, four information, the starting point address of IP header, IP header starting point port number, the service IP address number indicated by the payload, and the service port number indicated by the payload, is extracted from the "service access demand message", respectively.

[0038] And four information by which the extract was carried out [above-mentioned] is stored in four storage regions (field), an authorization starting point IP address field (ASIP), an authorization terminal point IP address field (ADIP), the authorization starting point port number field (ASPT), and the authorization terminal point port number field (ADPT), respectively, and an "access-permission entry" is created (step S4).

[0039] There is "the last access-permission time-of-day field (LATM)" which stores in an access-permission entry the time of day when using this entry and relaying a packet from a global-network 10 side to a local network 20 side at the end in addition to the four fields mentioned above, and when it is new creation, the time of day which created that access-permission entry is stored in the field concerned.

[0040] And the "access-permission entry" created as mentioned above is added to an "access permit list" (step S5).

[0041] An example of the access-permission entry generated by the processing mentioned above is shown in drawing 4 . The address which the global IP address of a device which transmitted the service access demand message, 131.113.82.1 [for example,], is stored in an authorization starting point IP address field (ASIP) in the entry concerned like illustration, and shows the destination of a service access demand message to an authorization terminal point IP address field (ADIP), for example, the global IP address currently assigned to the interface section 33 by the side of WAN of the gateway 30, and 210.139.255.223 It is stored. (Moreover, the port number of a device which transmitted the service access demand message to the authorization starting point port number field (ASPT), for example, 20010, It is stored and 5000 is further stored in the authorization terminal point port number field (ADPT) here [the port number and here] where the destination of a service access demand message is shown.) Moreover, 21:10:10 which is the time of day which created the entry is stored in the last access-permission time-of-day field (LATM).

[0042] The access-permission entry shown in drawing 4 is added to an access permit list. In addition, the access permit list concerned is managed by the access-control section 31, for example, is memorized by the storage section 35.

[0043] Next, it explains, referring to the flow chart shown in drawing 5 about actuation of the access-control section 33 by the WAN side interface section 33, when a data packet is received from global network 10.

[0044] First, a data packet is received from the WAN side interface section 33 (step SS 1). Four information is extracted for the starting point IP address (SIP) of IP header, the terminal point IP address (DIP) of IP header, the starting point port number (SPT) of a TCP/UDP header, and the terminal point

port number (DPT) of a TCP/UDP header from the data packet which received, respectively.
[0045] And with reference to the access permit list currently held at the storage section 35, ASIP is equal to SIP, ADIP is equal to DIP, ASPT is equal to SPT, and it checks about whether an access-permission entry with ADPT still more nearly equal to DPT exists. According to the result of the check concerned, it opts for authorization or refusal of passage to the data packet which received (step SS 2).
[0046] In the above-mentioned check, when all the fields are not in agreement, passage of a data packet is not permitted but this data packet is discarded (step SS 3).
[0047] On the other hand, when the access-permission entry all whose fields correspond exists in the above-mentioned check, passage of the data packet which received is permitted. Current time of day is stored in the last access-permission time-of-day field (LATM) of the corresponding access-permission entry at this time (step SS 4). In addition, current time of day here is time amount shown by the time management section which is managed by OS (operation system) of the gateway 30, and is usually called a system clock.
[0048] After updating the last access-permission time-of-day field, the data packet which received is transmitted to the address translation section 32 (step SS 5). And in the address translation section 32, the global IP address in IP header of a data packet is changed into the local IP address currently used inside the local network 20, and is transmitted to the LAN side interface section 34. Concretely, DIP and DPT are changed into the local IP address and port number of a device which actually offer service by the local network 20 side, respectively. It is transmitted to a local network 20 by the LAN side interface section 34, and the changed data packet is transmitted to the device which actually offers service.
[0049] When it is going to access the service currently offered by the local network 20 from the device by the side of global network 10 by the processing mentioned above, the starting point, the terminal point IP address and the starting point contained in IP header of a data packet, and TCP / UDP header received by the gateway 30, and terminal point port number information are extracted, it is based on a comparison result with the access permit list memorized by the extracted information and the storage section 35 concerned, and it is determined whether to permit or refuse access. When the access concerned is refused, a data packet is discarded, and when the access concerned is permitted conversely, the destination of a data packet is changed into the local IP address of a device which is used by the local network 20 and which carries out service provision by the address translation section 32, and is transmitted to a local network 20 side through the LAN side interface section 34.
[0050] For this reason, since only access from the attested device is permitted and access from the other device is refused when accessing the service currently offered by the local network 20 side from the device by the side of global network 10, the security nature of a fire wall improves, injustice can refuse access, and also access from the attested device is permitted and high service of convenience can be offered to the user of normal.
[0051] The access permit list formed of the access-permission entry of access permitted to the storage section 35 by processing mentioned above is memorized. In the gateway 30, a judgment whether based on the access permit list concerned, IP header of the received data packet, and TCP/UDP header information, the received data packet is transmitted to a local network 20 side is made. Since a new access-permission entry is created to the access whenever access is established, and it is added to an access permit list, it increases according to the number of accesses which the capacity of an access permit list received. Furthermore, in order that the access-permission entry about access which received authentication once may remain in the access permit list of the storage section 35 eternally even when the access is completed even if if it leaves an access-permission entry to an access permit list as it is, there is a security top problem. For this reason, it is necessary to delete that access-permission entry at any time to ended access.
[0052] Drawing 6 is a flow chart which shows the processing which deletes an access-permission entry based on the last access-permission time of day and threshold level time amount. Hereafter, the deletion of an access-permission entry is explained with reference to drawing 6 .
[0053] This deletion is the elapsed time tD from the last access-permission time of day to current (at the time of decision) time of day. Threshold level time amount TS set up beforehand It compares and is

elapsed time tD as a result of a comparison. Threshold level time amount TS When it exceeds, that access-permission entry is deleted from an access permit list. That is, even if it goes through fixed time amount from the last access, when there is no new access, the authorization to the access is canceled. In addition, this deletion is performed to the all entry in an access permit list for every fixed time amount of a certain.

[0054] As shown in drawing 6 , it is the value tf of an access-permission entry to the last access-permission time-of-day field (LATM) first. It is read (step SP 1). And the elapsed time tD (= t-tf) from the difference, i.e., last access-permission time of day, of the present time of day t and the time of day tf read from the last access-permission time-of-day field to current is calculated. The elapsed time tD concerned Threshold level time amount TS It is compared (step SP 2).

[0055] Elapsed time tD Threshold level time amount TS When small, nothing is processed to the access-permission entry (step SP 3). Elapsed time tD Threshold level time amount TS Equally, when larger, the access-permission entry is deleted from an access permit list (step SP 4).

[0056] It is the elapsed time tD from the last access time by the processing mentioned above. Predetermined threshold level time amount TS When it exceeds, the access-permission entry is deleted from an access permit list. That is, when it has gone through fixed time amount from the last access and there is no access, it is regarded as what ended the access, and an access-permission entry is deleted. In addition, threshold level time amount TS It can be set as a different value for every access-permission entry. For example, it is related with access to a WWW server, and is the threshold level time amount TS of an access-permission entry. Threshold level time amount TS of the access-permission entry set up short and concerning Telnet and FTP It can set up for a long time.

[0057] Drawing 7 is a flow chart which shows the processing which deletes the access-permission entry formed to the access from an access permit list, when the notice of access termination is received from the side to access. Hereafter, this deletion is explained, referring to drawing 7 .

[0058] Like illustration, a data packet is first received from the WAN side interface section 33 (step SQ1). Next, a judgment is made about whether the information (henceforth access termination information for convenience) which shows termination is included in the received data packet (step SQ2).

[0059] When access termination information is not included as a result of the decision concerned, the usual processing is performed to a data packet (step SQ3). On the other hand, when access termination information is included in the data packet as a result of the decision concerned, the access-permission entry according to the access concerned is deleted from an access permit list (step SQ4).

[0060] When access termination information is included in the data packet which received by the processing mentioned above, the access-permission entry formed when the access was established is deleted from an access permit list. For this reason, since the access-permission entry currently formed when access was completed according to this and that access was established is immediately deleted from an access permit list when termination of access is directed from the device by the side of global network 10, it can prevent that that entry is abused after access termination, and is desirable on security.

[0061] When a certain constant value is exceeded, it becomes impossible moreover, to store the number of the access-permission entries in an access permit list, since the resource of the gateway 30 is limited. For this reason, out of the access permit list currently held when an access-permission entry new in the situation of max [number / of access-permission entries] is added, an access-permission entry with the oldest value of the last access-permission time of day of an access-permission entry can be deleted, and a new access-permission entry can be added.

[0062] As mentioned above, although two kinds of entry deletion in the network connection control unit 30 of this operation gestalt, i.e., the gateway, was explained, entry deletion of the gateway 30 can also be performed by other processings, without being restricted to this. For example, terminating access is also considered based on decision of the processing which terminates access compulsorily based on decision of the gateway 30, or the device which actually provides the local network side with service.

[0063]

[Effect of the Invention] As explained above, according to the network connection control unit and its control approach of this invention, in the gateway equipped with the fire wall function, it is permitted that only the device by the side of the permitted global network accesses the service by the side of a local network, and a network user can use easily the service currently offered by a certain local network from the network of a migration place if needed. On the other hand, access from other users' device can be refused by setup of the fire wall of the gateway, and there is an advantage which can maintain the security level by the side of a local network.

[Translation done.]